配置、驗證Firepower裝置註冊並對其進行故障排除

目錄

簡介

本檔案將說明Firepower威脅防禦(FTD)和Firepower管理中心(FMC)之間連線的疑難排解程式。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- FTD軟體6.6.x和6.5.x
- FMC軟體6.6.x

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本檔案介紹受管FTD和受管FMC之間的連線(sftunnel)的運作、驗證和疑難排解程式。

資訊和示例基於FTD，但大多數概念也完全適用於NGIPS（7000/8000系列裝置）或ASA55xx上的FirePOWER模組。

FTD支援2種主要管理模式：

- 通過FMC實現開箱即用 — 也稱為遠端管理
- 通過Firepower裝置管理器(FDM)和/或Cisco Defense Orchestrator(CDO)進行開箱即用 — 也稱為本地管理

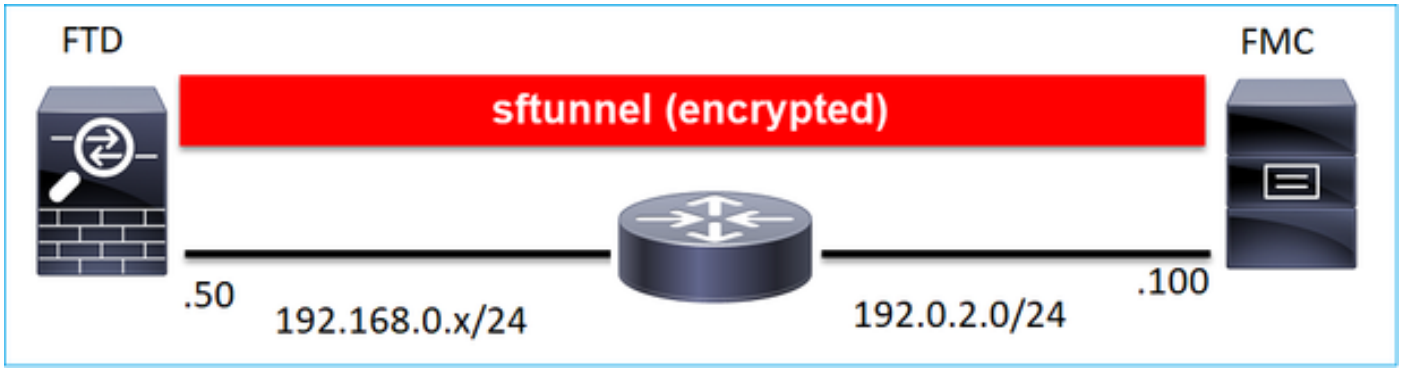
在遠端管理的情況下，FTD需要首先註冊到使用稱為裝置註冊的進程的FMC。

完成註冊後，FTD和FMC會建立一個名為sftunnel（名稱從Sourcefire通道派生）的安全通道。

設計選項

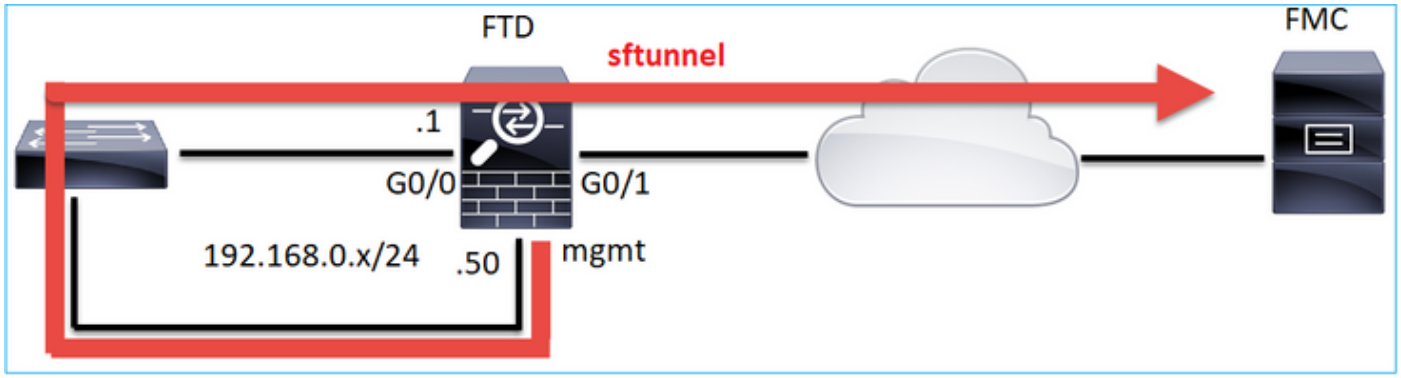
從設計的角度來看，FTD - FMC可以位於同一個L3子網中：

或由不同的網路分隔：



192.0.2.0

註:sftunnel也可通過FTD本身。不建議使用此設計。原因是FTD資料平面問題可能會中斷FTD和FMC之間的通訊。



通過sftunnel交換什麼資訊？

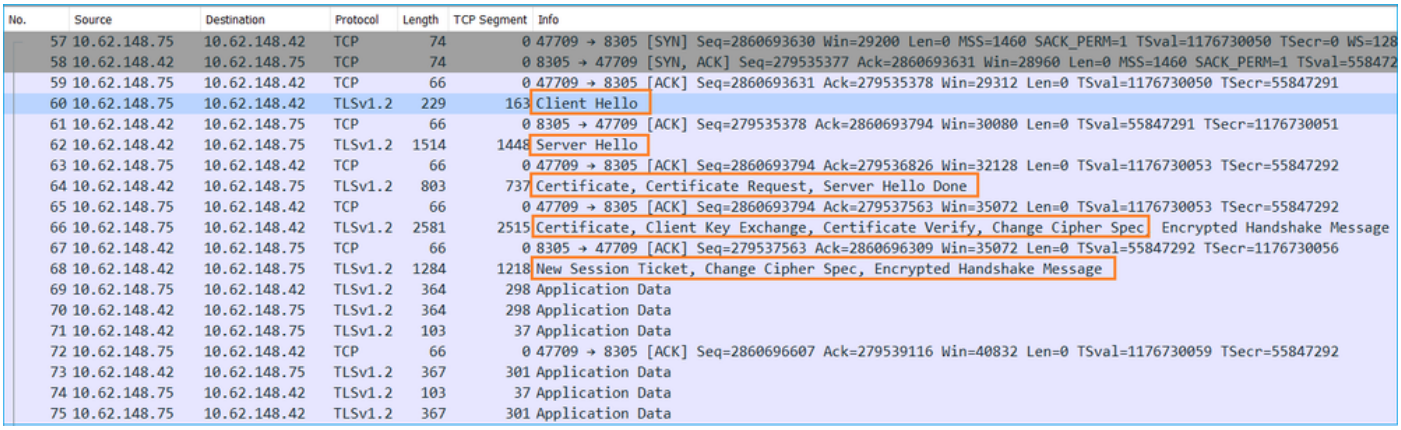
此清單包含通過sftunnel傳輸的大部分資訊：

- 裝置心跳(keepalive)
- 時間同步(NTP)
- 事件（連線、入侵/IPS、檔案、SSL等）

- 惡意軟體查詢
- 運行狀況事件/警報
- 使用者和組資訊（用於身份策略）
- FTD HA狀態資訊
- FTD叢集狀態資訊
- 安全智慧(SI)資訊/事件
- Threat Intelligence Director(TID)資訊/事件
- 捕獲的檔案
- 網路發現事件
- 策略捆綁包（策略部署）
- 軟體升級捆綁包
- 軟體補丁捆綁包
- VDB
- SRU

sftunnel使用什麼協定/埠？

sftunnel使用TCP端口8305。在後端是TLS通道：



No.	Source	Destination	Protocol	Length	TCP Segment	Info
57	10.62.148.75	10.62.148.42	TCP	74	0	47709 → 8305 [SYN] Seq=2860693630 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1176730050 TSecr=0 WS=128
58	10.62.148.42	10.62.148.75	TCP	74	0	8305 → 47709 [SYN, ACK] Seq=279535377 Ack=2860693631 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=558472
59	10.62.148.75	10.62.148.42	TCP	66	0	47709 → 8305 [ACK] Seq=2860693631 Ack=279535378 Win=29312 Len=0 TSval=1176730050 TSecr=55847291
60	10.62.148.75	10.62.148.42	TLSv1.2	229	163	Client Hello
61	10.62.148.42	10.62.148.75	TCP	66	0	8305 → 47709 [ACK] Seq=279535378 Ack=2860693794 Win=30080 Len=0 TSval=55847291 TSecr=1176730051
62	10.62.148.42	10.62.148.75	TLSv1.2	1514	1448	Server Hello
63	10.62.148.75	10.62.148.42	TCP	66	0	47709 → 8305 [ACK] Seq=2860693794 Ack=279536826 Win=32128 Len=0 TSval=1176730053 TSecr=55847292
64	10.62.148.42	10.62.148.75	TLSv1.2	803	737	Certificate, Certificate Request, Server Hello Done
65	10.62.148.75	10.62.148.42	TCP	66	0	47709 → 8305 [ACK] Seq=2860693794 Ack=279537563 Win=35072 Len=0 TSval=1176730053 TSecr=55847292
66	10.62.148.75	10.62.148.42	TLSv1.2	2581	2515	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
67	10.62.148.42	10.62.148.75	TCP	66	0	8305 → 47709 [ACK] Seq=279537563 Ack=2860696309 Win=35072 Len=0 TSval=55847292 TSecr=1176730056
68	10.62.148.42	10.62.148.75	TLSv1.2	1284	1218	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
69	10.62.148.75	10.62.148.42	TLSv1.2	364	298	Application Data
70	10.62.148.42	10.62.148.75	TLSv1.2	364	298	Application Data
71	10.62.148.42	10.62.148.75	TLSv1.2	103	37	Application Data
72	10.62.148.75	10.62.148.42	TCP	66	0	47709 → 8305 [ACK] Seq=2860696607 Ack=279539116 Win=40832 Len=0 TSval=1176730059 TSecr=55847292
73	10.62.148.42	10.62.148.75	TLSv1.2	367	301	Application Data
74	10.62.148.75	10.62.148.42	TLSv1.2	103	37	Application Data
75	10.62.148.75	10.62.148.42	TLSv1.2	367	301	Application Data

如何變更FTD上的Sftunnel TCP連線埠？

<#root>

>

configure network management-port 8306

Management port changed to 8306.

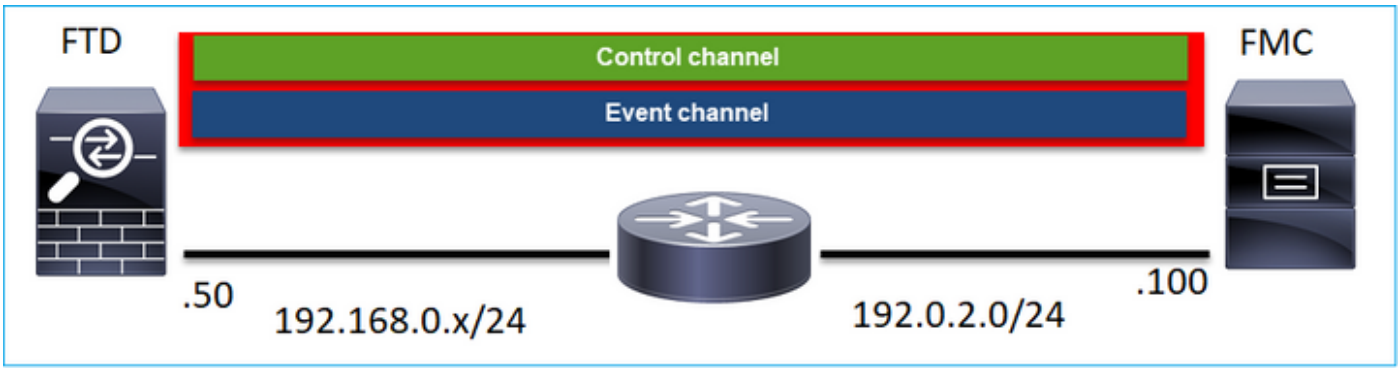
注意：在這種情況下，您還必須更改FMC上的埠(Configuration > Management Interfaces > Shared Settings)。這會影響已註冊到同一FMC的所有其他裝置。思科強烈建議您保留遠端管理埠的預設設定，但如果管理埠與網路中的其他通訊衝突，則可以選擇不同的埠。如果更改管

理埠，必須為部署中需要相互通訊的所有裝置更改該埠。

sftunnel建立了多少個連線？

sftunnel建立2個連線（通道）：

- 控制通道
- 事件通道



哪個裝置啟動每個通道？

這取決於具體情況。檢查文檔其餘部分中描述的場景。

設定

註冊基礎知識

FTD CLI

在FTD上，裝置註冊的基本語法為：

> configure manager add <FMC Host> <Registration Key> <NAT ID>

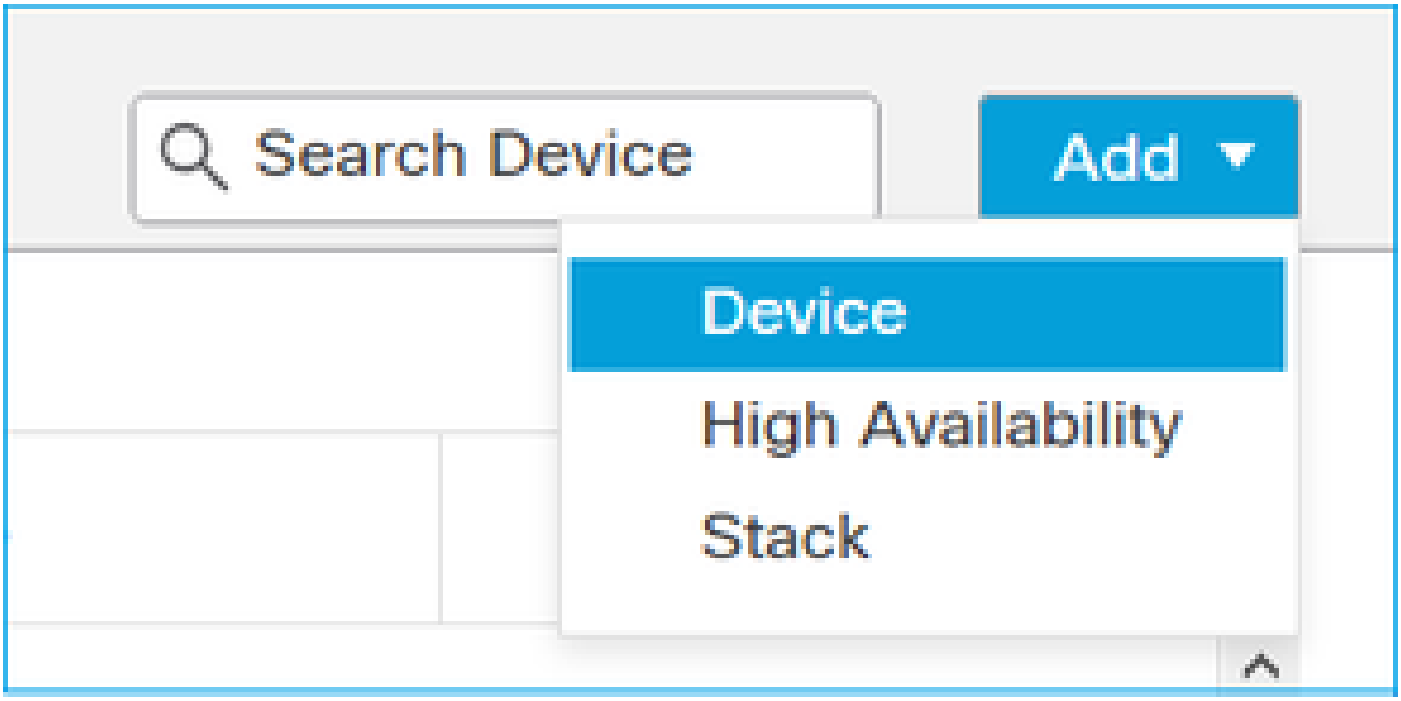
價值	說明
FMC主機	可以是： • 主機名 • ipv4位址 • ipv6地址 • DONTRESOLVE

註冊金鑰	這是用於裝置註冊的共用金鑰字母數字字串（2到36個字元）。只允許使用字母數字、連字元(-)、下劃線(_)和句點(.)。
NAT ID	當一端未指定IP地址時，在FMC和裝置之間的註冊過程中使用的字母數字字串。在FMC上指定相同的NAT ID。

有關其他詳細資訊，請檢視Cisco Firepower威脅防禦命令參考

FMC UI

在FMC上，導航到Devices > Device Management。選擇Add > Device



Add Device

Host:*

Display Name:

Registration Key:*

Domain:

Select Domain

Group:

None

Access Control Policy:*

Smart Licensing

- [ ] Malware
- [ ] Threat
- [ ] URL Filtering

Advanced

Unique NAT ID:*

- [x] Transfer Packets

FTD CLI

> configure manager add <FMC Static IP> <Registration Key>

舉例來說：

<#root>

>

configure manager add 10.62.148.75 Cisco-123

Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

背景資訊

輸入FTD命令後，FTD會每20秒嘗試連線到FMC，但由於尚未設定FMC，因此它會使用TCP RST回覆：

<#root>

>

capture-traffic

Please choose domain to capture traffic from:
  0 - eth0
  1 - Global

Selection?

0

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:

-n host 10.62.148.75

HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
18:53:33.365513 IP 10.62.148.42.46946 > 10.62.148.75.8305: Flags

[S]

, seq 2274592861, win 29200, options [mss 1460,sackOK,TS val 55808298 ecr 0,nop,wscale 7], length 0
18:53:33.365698 IP 10.62.148.75.8305 > 10.62.148.42.46946: Flags

[R.]

```
, seq 0, ack 2274592862, win 0, length 0
18:53:53.365973 IP 10.62.148.42.57607 > 10.62.148.75.8305: Flags
```

[S]

```
, seq 1267517632, win 29200, options [mss 1460,sackOK,TS val 55810298 ecr 0,nop,wscale 7], length 0
18:53:53.366193 IP 10.62.148.75.8305 > 10.62.148.42.57607: Flags
```

[R.]

```
, seq 0, ack 1267517633, win 0, length 0
18:54:13.366383 IP 10.62.148.42.55484 > 10.62.148.75.8305: Flags
```

[S]

```
, seq 4285875151, win 29200, options [mss 1460,sackOK,TS val 55812298 ecr 0,nop,wscale 7], length 0
18:54:13.368805 IP 10.62.148.75.8305 > 10.62.148.42.55484: Flags
```

[R.]

```
, seq 0, ack 4285875152, win 0, length 0
```

裝置註冊狀態：

<#root>

```
>
```

show managers

```
Host                    : 10.62.148.75
Registration Key        : ****
Registration            : pending
RPC Status              :
Type                    : Manager
Host                    : 10.62.148.75
Registration            : Pending
```

FTD偵聽連線埠TCP 8305:

<#root>

```
admin@vFTD66:~$
```

netstat -na | grep 8305

```
tcp        0      0 10.62.148.42:
```

8305

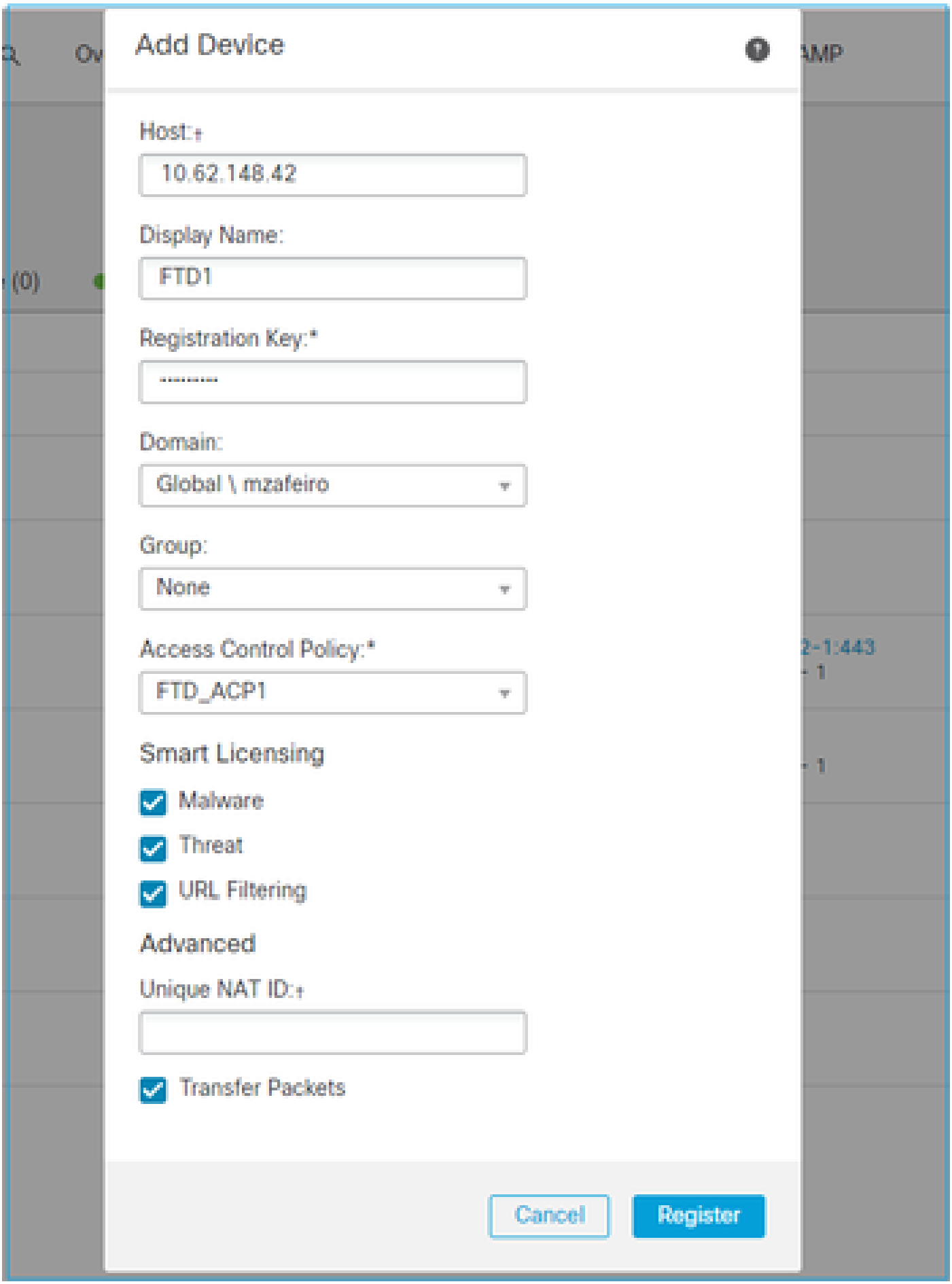
```
       0.0.0.0:*
```

LISTEN

FMC UI

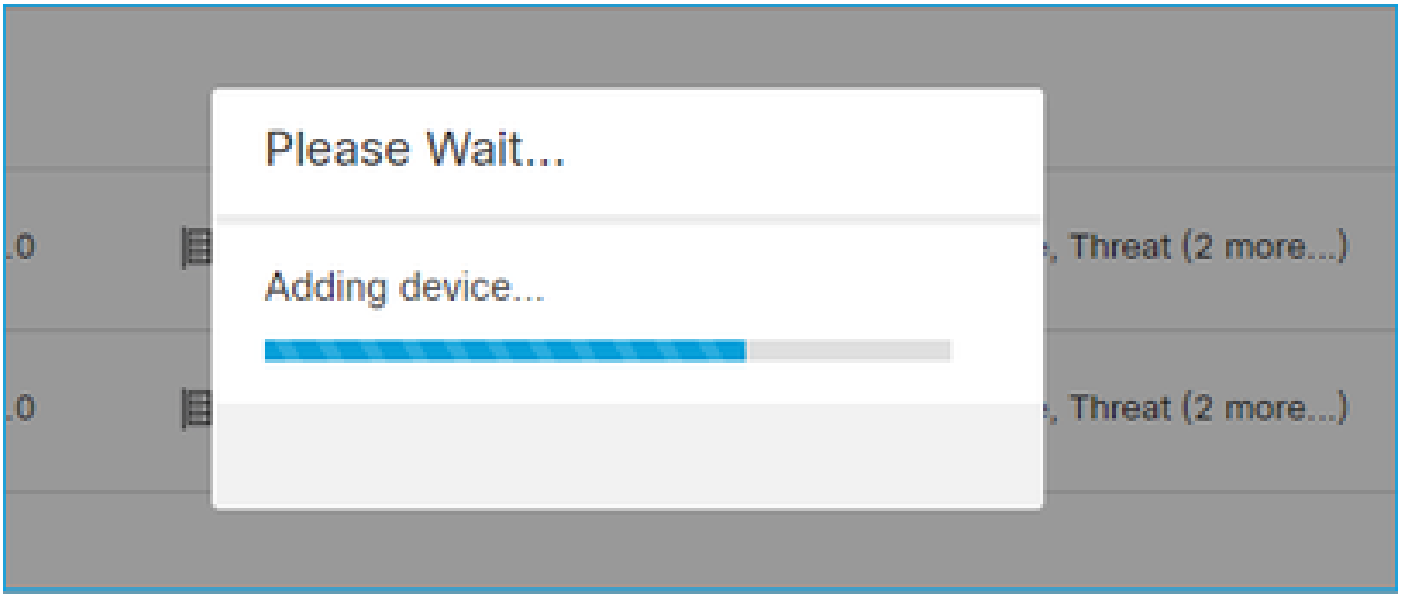
在這種情況下，請指定：

- 主機（FTD的IP位址）
- 顯示名稱
- 註冊金鑰（必須與FTD上設定的金鑰相符）
- 訪問控制策略
- 域
- 智慧許可資訊


Add Device
Host:*
10.62.148.42
Display Name:
FTD1
Registration Key:*
Domain:
Global \ mzafeiro
Group:
None
Access Control Policy:*
FTD_ACP1
Smart Licensing
Malware
Threat
URL Filtering
Advanced
Unique NAT ID:*
Transfer Packets
Cancel
Register

選擇註冊

註冊過程開始：



FMC開始偵聽埠TCP 8305:

<#root>

admin@FMC2000-2:~$

netstat -na | grep 8305

tcp 0 0 10.62.148.75:

8305

0.0.0.0:*

LISTEN

FMC在後台發起TCP連線：

<#root>

```
20:15:55.437434 IP 10.62.148.42.49396 > 10.62.148.75.8305: Flags [S], seq 655146775, win 29200, options
20:15:55.437685 IP 10.62.148.75.8305 > 10.62.148.42.49396: Flags [R.], seq 0, ack 655146776, win 0, len
20:16:00.463637 ARP, Request who-has 10.62.148.42 tell 10.62.148.75, length 46
20:16:00.463655 ARP, Reply 10.62.148.42 is-at 00:50:56:85:7b:1f, length 28
20:16:08.342057 IP
```

10.62.148.75

.50693 > 10.62.148.42.8305: Flags

[S]

```
, seq 2704366385, win 29200, options [mss 1460,sackOK,TS val 1181294721 ecr 0,nop,wscale 7], length 0
20:16:08.342144 IP 10.62.148.42.8305 > 10.62.148.75.50693: Flags
```

[S.]

```
, seq 1829769842,
```

ack

```
 2704366386, win 28960, options [mss 1460,sackOK,TS val 56303795 ecr 1181294721,nop,wscale 7], length 0
20:16:08.342322 IP 10.62.148.75.50693 > 10.62.148.42.8305: Flags [.],
```

ack

```
 1, win 229, options [nop,nop,TS val 1181294722 ecr 56303795], length 0
20:16:08.342919 IP 10.62.148.75.50693 > 10.62.148.42.8305: Flags [P.], seq 1:164, ack 1, win 229, optio
20:16:08.342953 IP 10.62.148.42.8305 > 10.62.148.75.50693: Flags [.], ack 164, win 235, options [nop,no
```

已建立sftunnel控制通道：

<#root>

```
admin@FMC2000-2:~$
```

netstat -na | grep 8305

```
tcp        0      0 10.62.148.75:8305       0.0.0.0:*               LISTEN
tcp        0      0
```

10.62.148.75:50693   10.62.148.42:8305

ESTABLISHED

<#root>

```
>
```

sftunnel-status

```
SFTUNNEL Start Time: Sat Apr 18 20:14:20 2020

        Both IPv4 and IPv6 connectivity is supported
        Broadcast count = 4
        Reserved SSL connections: 0
        Management Interfaces: 1
        eth0 (control events) 10.62.148.42,

**********************

**RUN STATUS****ksec-fs2k-2-mgmt.cisco.com*************
        Cipher used = AES256-GCM-SHA384 (strength:256 bits)
```

ChannelA Connected: Yes, Interface eth0

ChannelB Connected: No

```
        Registration: Completed.
        IPv4 Connection to peer '10.62.148.75' Start Time: Sat Apr 18 20:16:08 2020


PEER INFO:
        sw_version 6.6.0
        sw_build 90
        Management Interfaces: 1
        eth0 (control events) 10.62.148.75,
```

Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.62.148.75' via '10.62.14

Peer channel Channel-B is not valid

幾分鐘後，建立事件通道。事件通道的發起者可以是兩端。在本例中，它是FMC:

<#root>

20:21:15.347587 IP 10.62.148.75.43957 > 10.62.148.42.8305: Flags

[S]

, seq 3414498581, win 29200, options [mss 1460,sackOK,TS val 1181601702 ecr 0,nop,wscale 7], length 0
20:21:15.347660 IP 10.62.148.42.8305 > 10.62.148.75.43957: Flags

[S.]

, seq 2735864611,

ack

 3414498582, win 28960, options [mss 1460,sackOK,TS val 56334496 ecr 1181601702,nop,wscale 7], length 0
20:21:15.347825 IP 10.62.148.75.43957 > 10.62.148.42.8305: Flags [.],

ack

 1, win 229, options [nop,nop,TS val 1181601703 ecr 56334496], length 0
20:21:15.348415 IP 10.62.148.75.43957 > 10.62.148.42.8305: Flags [P.], seq 1:164, ack 1, win 229, optio

隨機源埠表示連線啟動器：

<#root>

admin@FMC2000-2:~$

netstat -na | grep 10.62.148.42

tcp   0   0 10.62.148.75:

50693

      10.62.148.42:8305   ESTABLISHED
tcp   0   0 10.62.148.75:

43957

10.62.148.42:8305 ESTABLISHED

如果Event channel由FTD啟動，則輸出為：

<#root>

admin@FMC2000-2:~$

netstat -na | grep 10.62.148.42

tcp 0 0 10.62.148.75:

58409

10.62.148.42:8305 ESTABLISHED
tcp 0 0 10.62.148.75:8305 10.62.148.42:

46167

ESTABLISHED

在FTD一側：

<#root>

>

sftunnel-status

SFTUNNEL Start Time: Sat Apr 18 20:14:20 2020

Both IPv4 and IPv6 connectivity is supported
Broadcast count = 6
Reserved SSL connections: 0
Management Interfaces: 1
eth0 (control events) 10.62.148.42,

****

RUN STATUS**ksec-fs2k-2-mgmt.cisco.com**********
Cipher used = AES256-GCM-SHA384 (strength:256 bits)

ChannelA Connected: Yes,

Interface eth0
Cipher used = AES256-GCM-SHA384 (strength:256 bits)

ChannelB Connected: Yes,

Interface eth0
Registration: Completed.
IPv4 Connection to peer '10.62.148.75' Start Time: Sat Apr 18 20:16:08 2020

```
PEER INFO:
        sw_version 6.6.0
        sw_build 90
        Management Interfaces: 1
        eth0 (control events) 10.62.148.75,


 Peer channel Channel-A is valid  type (CONTROL), using 'eth0', connected to '10.62.148.75' via '10.62.1
        Peer channel Channel-B is valid  type (EVENT), using 'eth0', connected to '10.62.148.75' via '10
```

<#root>

>

show managers

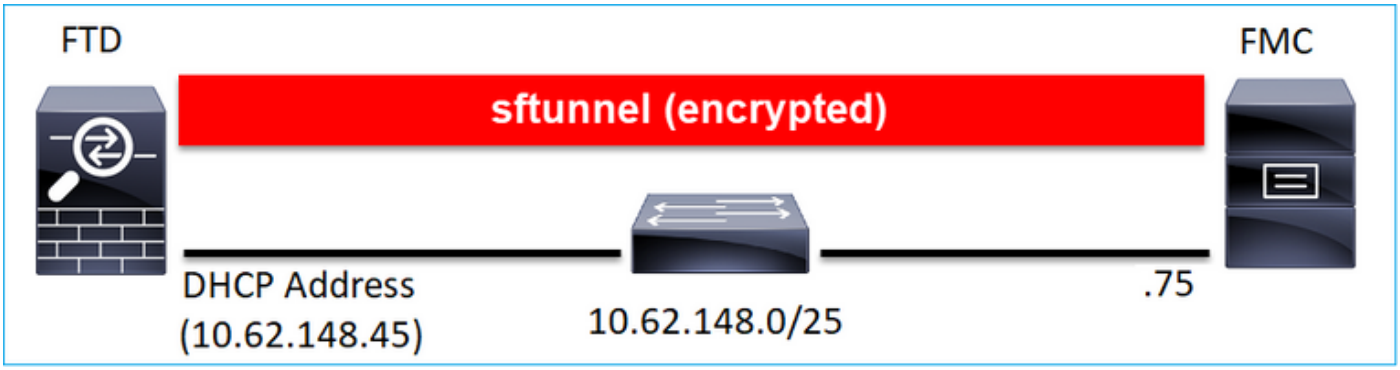
Type : Manager
Host : 10.62.148.75

Registration : Completed

>

案例 2.FTD DHCP IP位址 — FMC靜態IP位址

在此案例中，FTD管理介面從DHCP伺服器取得其IP位址：



FTD CLI

必須指定NAT ID:

> configure manager add <FMC Static IP> <Registration Key> <NAT ID>

舉例來說：

<#root>

```
>

configure manager add 10.62.148.75 Cisco-123 nat123

Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
```

FTD註冊狀態：

```
<#root>

>

show managers

Host                    : 10.62.148.75
Registration Key        : ****

Registration            : pending

RPC Status              :
Type                    : Manager
Host                    : 10.62.148.75
Registration            : Pending
```

FMC UI

在這種情況下，請指定：

- 顯示名稱
- 註冊金鑰（必須與FTD上設定的金鑰相符）
- 訪問控制策略
- 域
- 智慧許可資訊
- NAT ID(如果未指定Host，則需要。它必須與FTD上設定的專案相符)

Add Device

Host:*

empty

Display Name:

FTD1

Registration Key:*

Domain:

Global \ mzafeiro

Group:

None

Access Control Policy:*

FTD_ACP1

Smart Licensing

- [x] Malware
- [x] Threat
- [x] URL Filtering

Advanced

Unique NAT ID:*

nat123

- [x] Transfer Packets

在這種情況下，由誰啟動sftunnel?

FTD會啟動兩個通道連線：

<#root>

```
ftd1:/home/admin#
netstat -an | grep 148.75
tcp        0      0 10.62.148.45:
40273
      10.62.148.75:8305       ESTABLISHED
tcp        0      0 10.62.148.45:
39673
      10.62.148.75:8305       ESTABLISHED
```

案例 3.FTD靜態IP地址 — FMC DHCP IP地址

<#root>

```
>
configure manager add DONTRESOLVE Cisco-123 nat123
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
>
```

注意：使用DONTRESOLVE時，需要NAT ID。

FMC UI

在這種情況下，請指定：

- FTD IP位址
- 顯示名稱
- 註冊金鑰（必須與FTD上設定的金鑰相符）
- 訪問控制策略
- 域
- 智慧許可資訊
- NAT ID（必須與FTD上設定的那個相符）

Add Device

Host:*

10.62.148.42

Display Name:

FTD1

Registration Key:*

.....

Domain:

Global \ mzafeiro

Group:

None

Access Control Policy:*

FTD_ACP1

Smart Licensing

- [x] Malware
- [x] Threat
- [x] URL Filtering

Advanced

Unique NAT ID:*

nat123

- [x] Transfer Packets

- FMC啟動控制通道。
- 事件通道可以由任一端啟動。

<#root>

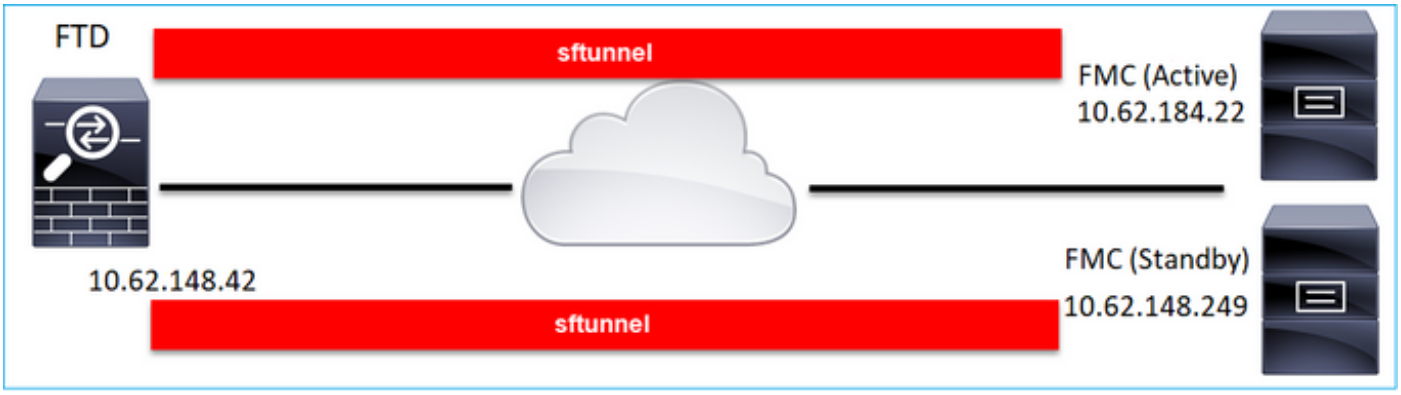
```
root@FMC2000-2:/Volume/home/admin#

netstat -an | grep 148.42

tcp        0      0 10.62.148.75:

50465

      10.62.148.42:8305       ESTABLISHED
tcp        0      0 10.62.148.75:

48445

      10.62.148.42:8305       ESTABLISHED
```

案例 4.FTD註冊FMC HA

在FTD上，僅設定作用中FMC:

<#root>

```
>

configure manager add 10.62.184.22 cisco123

Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

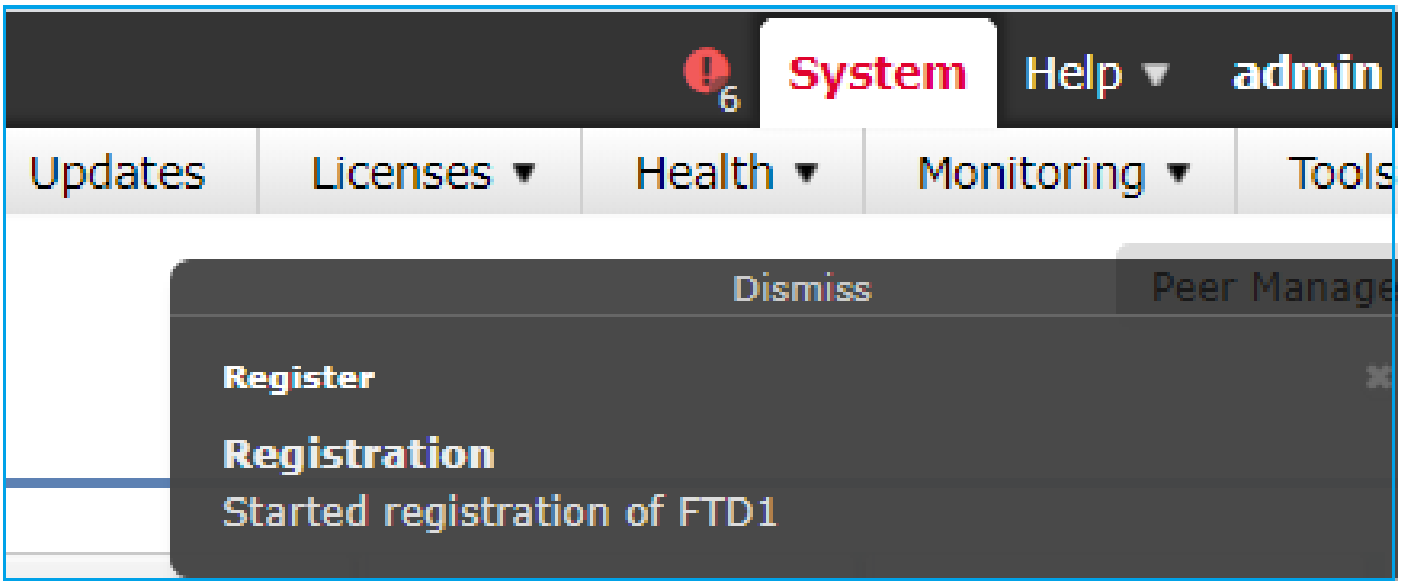


註：確保TCP埠8305流量允許從FTD傳輸到兩個FMC。

首先，建立到活動FMC的sftunnel:

```
<#root>

>

show managers

Type                    : Manager
Host                    :

10.62.184.22

Registration            : Completed
```

幾分鐘後，FTD開始註冊待命FMC:




```
<#root>

>

show managers

Type                    : Manager
Host                    :

10.62.184.22

Registration            : Completed


Type                    : Manager
```

```
Host                          :
10.62.148.249
Registration                  : Completed
```

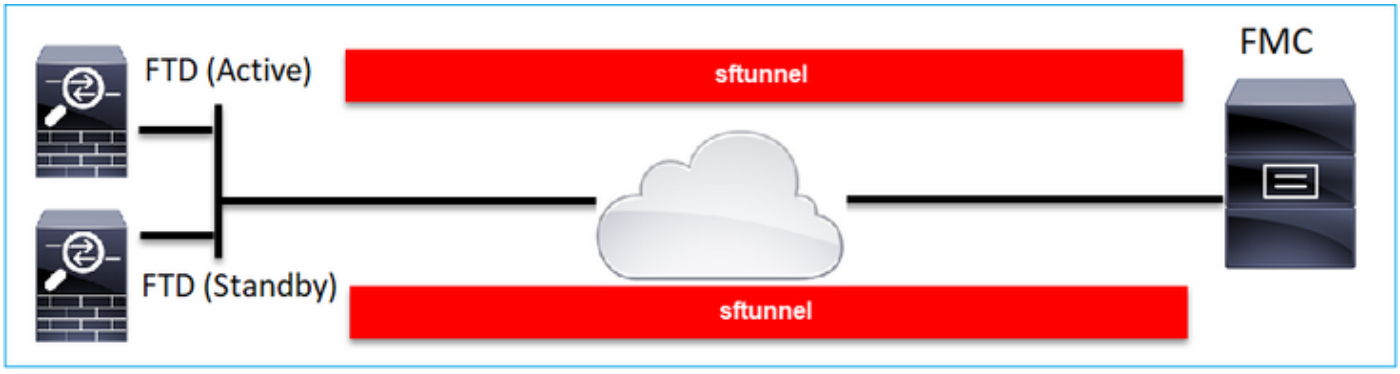
在FTD後端中，建立2個控制通道（1個對應每個FMC）和2個事件通道（1個對應每個FMC）：

<#root>

```
ftd1:/home/admin#
netstat -an | grep 8305

tcp        0      0 10.62.148.42:8305       10.62.184.22:36975      ESTABLISHED
tcp        0      0 10.62.148.42:42197      10.62.184.22:8305       ESTABLISHED
tcp        0      0 10.62.148.42:8305       10.62.148.249:45373     ESTABLISHED
tcp        0      0 10.62.148.42:8305       10.62.148.249:51893     ESTABLISHED
```

案例 5.FTD HA

在FTD HA的情況下，每個裝置都有一個前往FMC的獨立通道：

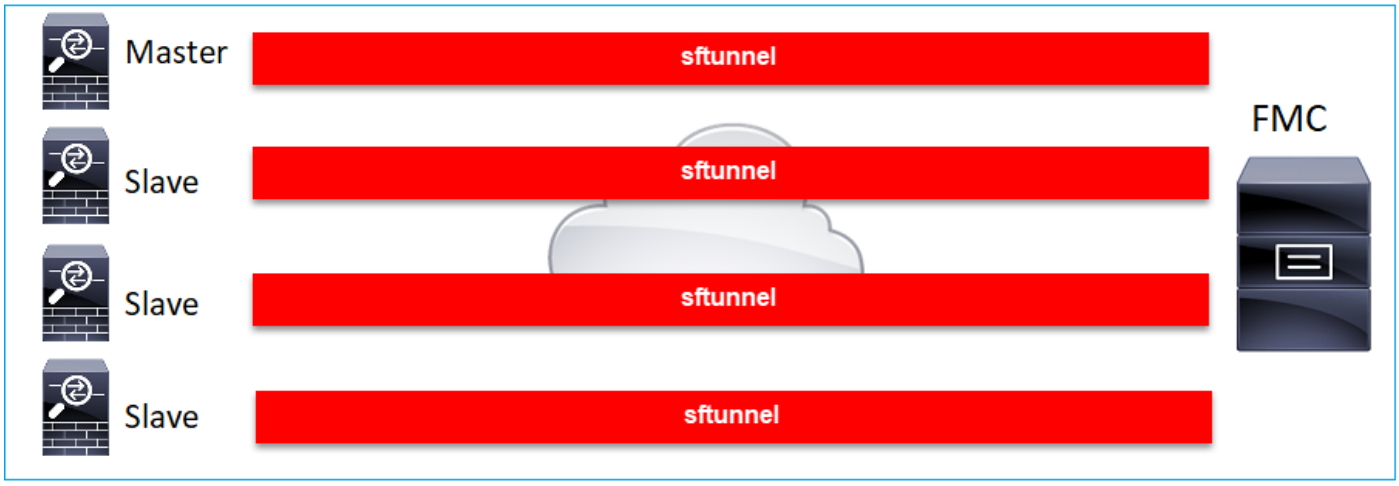


您獨立註冊兩個FTD，然後從FMC形成FTD HA。有關更多詳細資訊，請檢視：

- 在 Firepower 設備上設定 FTD 高可用性
- Firepower威脅防禦的高可用性

案例 6.FTD叢集

對於FTD集群，每個單元都有到FMC的獨立隧道。自6.3 FMC版本起，您只需將FTD控制單元註冊到FMC。然後FMC處理其餘單元並自動發現+註冊它們。

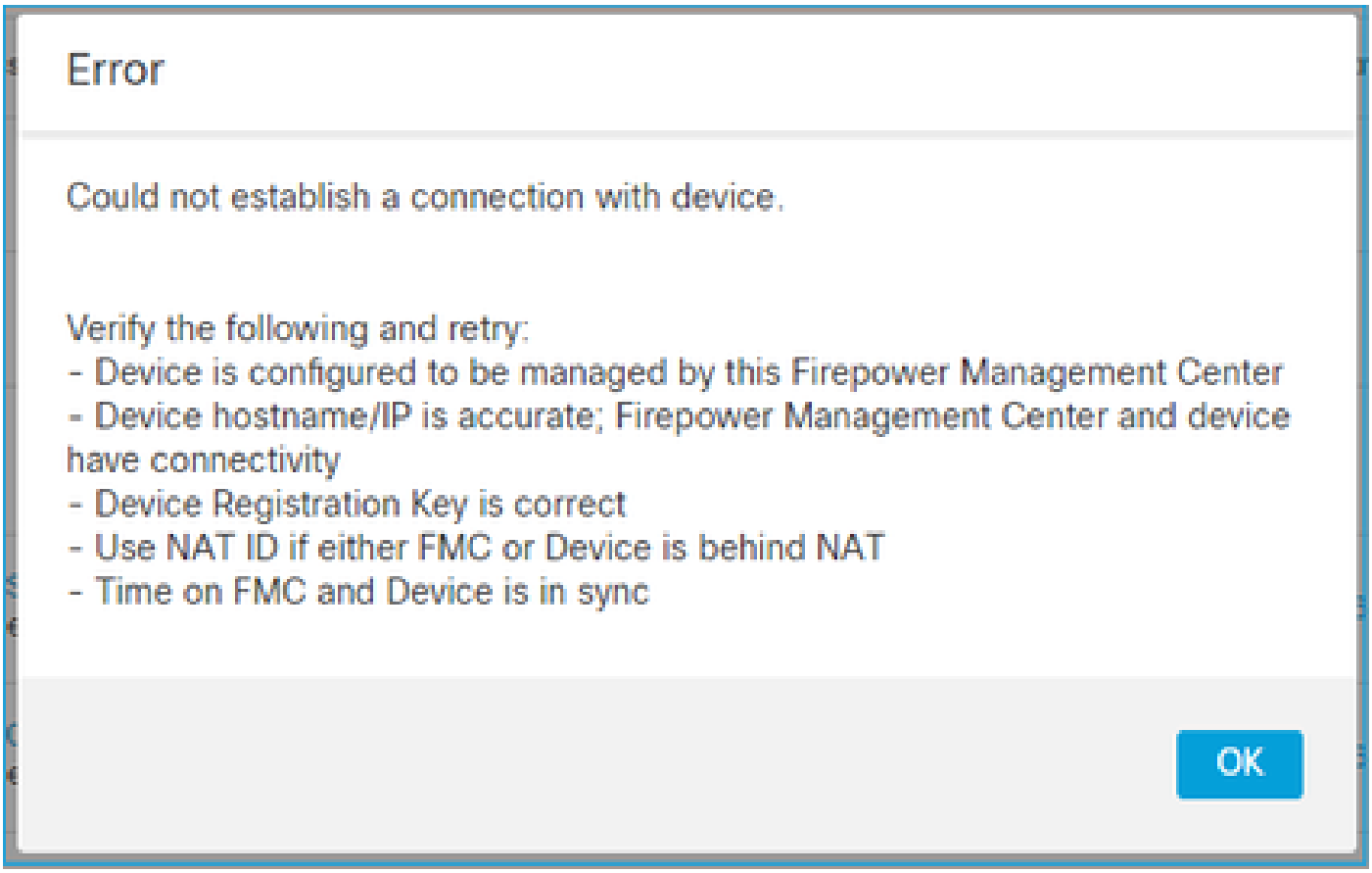


注意：我們建議新增控制單元以獲得最佳效能，但您可以新增集群中的任何單元。有關其他詳細資訊，請檢查：建立Firepower威脅防禦群集

常見問題疑難解答

1. FTD CLI上的語法無效

如果FTD上的語法無效，且註冊嘗試失敗，則FMC UI會顯示非常一般的錯誤訊息：



在此命令中，關鍵字key是註冊金鑰，而cisco123是NAT ID。在技術上不存在關鍵字時，新增關鍵字鍵非常常見：

```
<#root>

>

configure manager add 10.62.148.75 key cisco123

Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

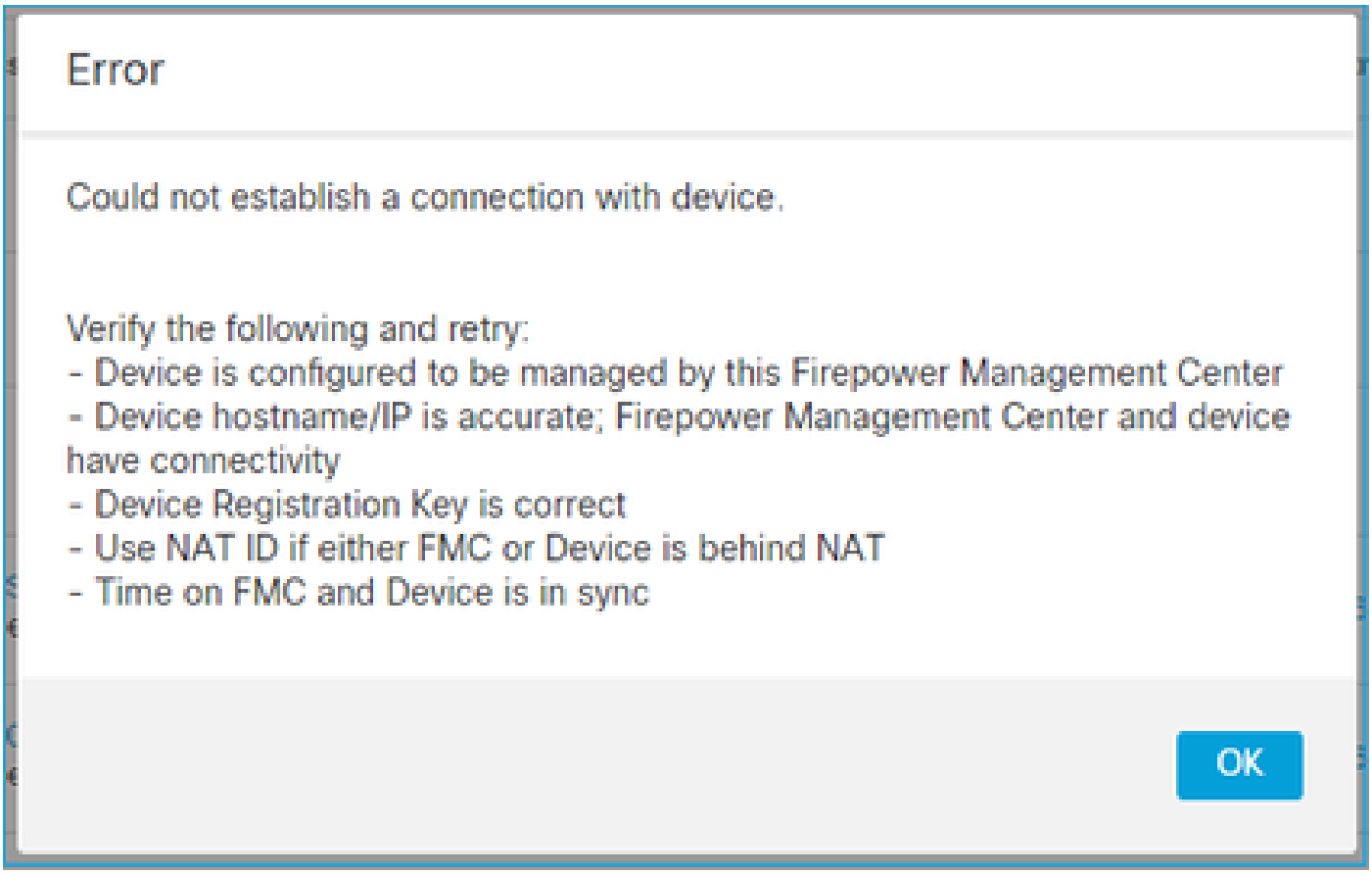
建議的操作

使用正確的語法，不要使用不存在的關鍵字。

```
<#root>

>

configure manager add 10.62.148.75 cisco123

Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

2. FTD之間的註冊金鑰不匹配 — FMC

FMC UI顯示：



建議的操作

在FTD上，檢查/ngfw/var/log/messages檔案以瞭解驗證問題。

方法1 — 檢查過去的日誌

<#root>

```
>

system support view-files

Type a sub-dir name to list its contents:

s


Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
>
```

messages
Apr

19 04:02:05 vFTD66 syslog-ng[1440]: Configuration reload request received, reloading configuration;
Apr 19 04:02:07 vFTD66 SF-IMS[3116]: [3116] pm:control [INFO] ControlHandler auditing message->type 0x9
w/usr/bin/perl /ngfw/usr/local/sf/bin/run_hm.pl --persistent', pid 19455 (uid 0, gid 0)

/authenticate

Apr 19 20:17:14 vFTD66 SF-IMS[18974]: [19131] sftunneld:sf_ssl [WARN] Accept:

Failed to authenticate peer '10.62.148.75' <- The problem

方法2 — 檢查活動日誌

<#root>

>

expert
ftd1:~$

sudo su

Password:
ftd1::/home/admin#

tail -f /ngfw/var/log/messages

在FTD上，檢查/etc/sf/sftunnel.conf檔案的內容，以確保註冊金鑰正確：

<#root>

ftd1:~$

cat /etc/sf/sftunnel.conf | grep reg_key

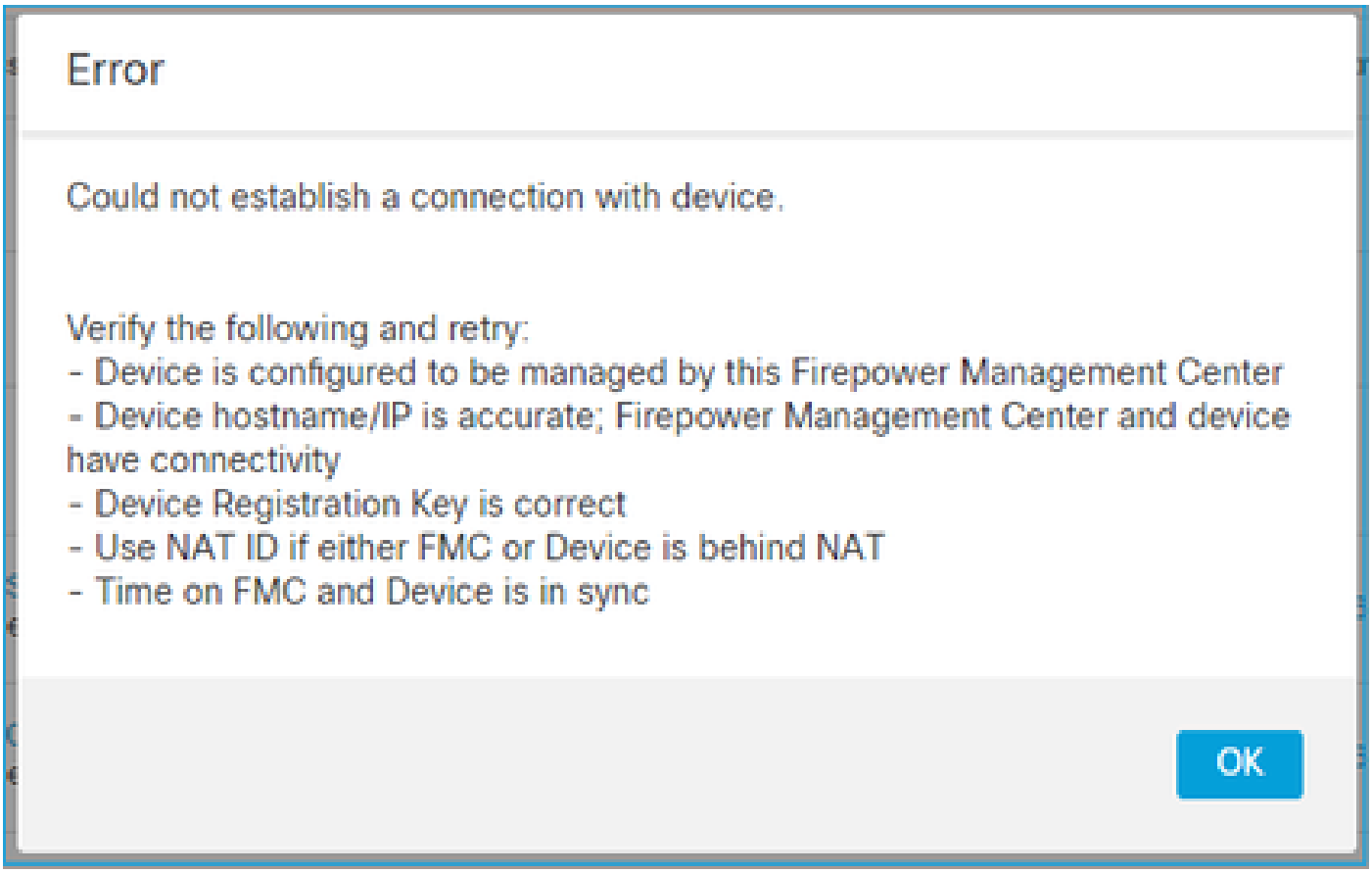
reg_key

cisco-123

;

3. FTD - FMC之間的連線問題

FMC UI顯示：



建議的操作

- 確保路徑中沒有阻止流量的裝置（例如防火牆）(TCP 8305)。在FMC HA的情況下，確保允許到TCP連線埠8305的流量流向兩個FMC。
- 捕獲以驗證雙向通訊。在FTD上使用capture-traffic 命令。確儲存在TCP三次握手，並且沒有TCP FIN或RST資料包。

```
<#root>

>

capture-traffic


Please choose domain to capture traffic from:
  0 - eth0
  1 - Global

Selection?

0


Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:

-n host 10.62.148.75

HS_PACKET_BUFFER_SIZE is set to 4.
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
20:56:09.393655 IP 10.62.148.42.53198 > 10.62.148.75.8305: Flags
```

[S]

```
, seq 3349394953, win 29200, options [mss 1460,sackOK,TS val 1033596 ecr 0,nop,wscale 7], length 0
20:56:09.393877 IP 10.62.148.75.8305 > 10.62.148.42.53198: Flags
```

[R.]

```
, seq 0, ack 3349394954, win 0, length 0
20:56:14.397412 ARP, Request who-has 10.62.148.75 tell 10.62.148.42, length 28
20:56:14.397602 ARP, Reply 10.62.148.75 is-at a4:6c:2a:9e:ea:10, length 46
```

同樣，在FMC上進行捕獲以確保雙向通訊：

<#root>

```
root@FMC2000-2:/var/common#
```

tcpdump -i eth0 host 10.62.148.42 -n -w sftunnel.pcap

還建議以pcap格式匯出捕獲並檢查資料包內容：

<#root>

```
ftd1:/home/admin#
```

tcpdump -i eth0 host 10.62.148.75 -n -w tunnel.pcap

```
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

可能原因:

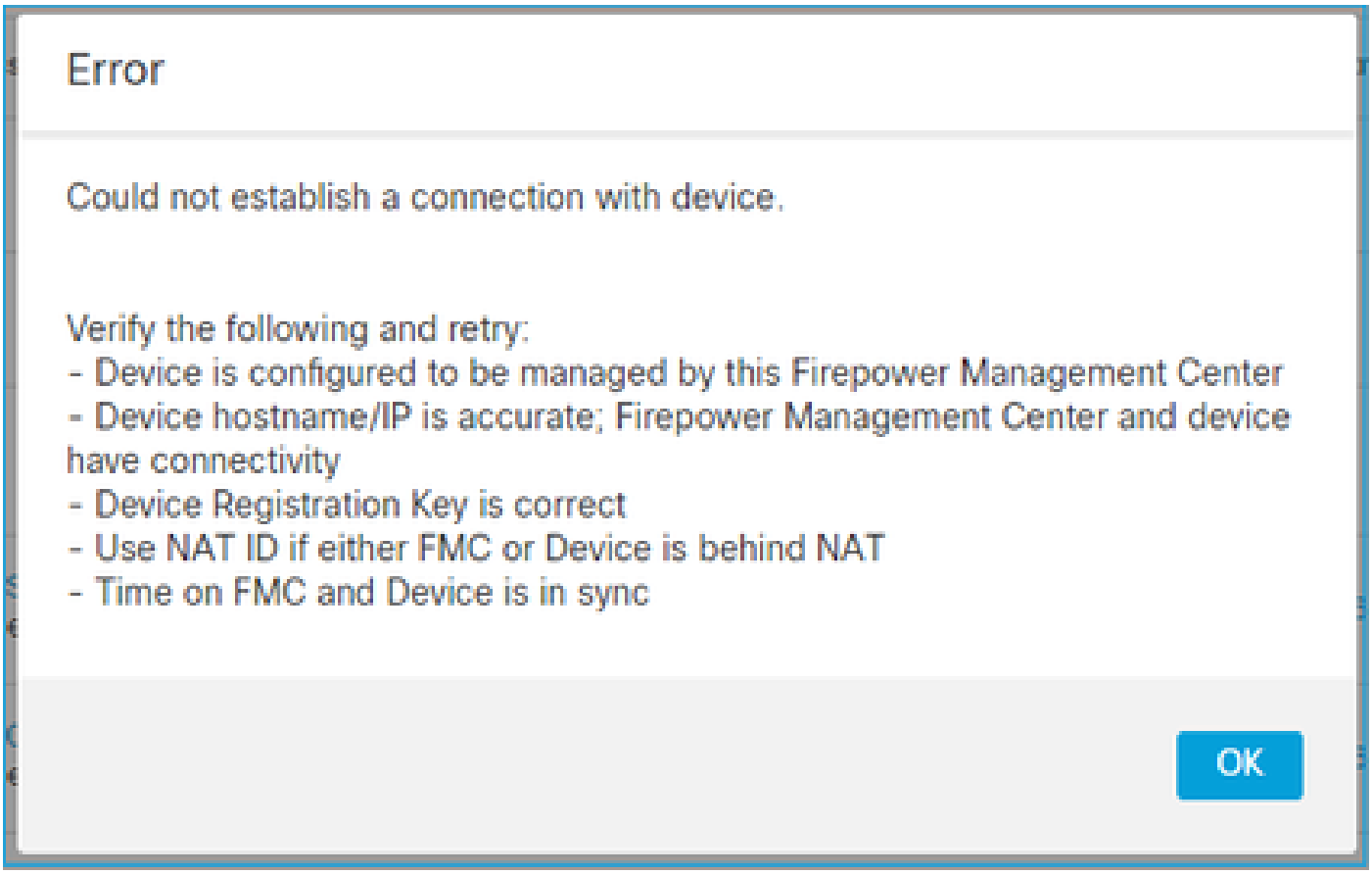
- FMC未新增FTD裝置。
- 路徑中的裝置（例如防火牆）阻止或修改流量。
- 封包在路徑中未正確路由。
- FTD或FMC上的sftunnel程式關閉（檢查案例6）
- 路徑中存在MTU問題（檢查案例）。

對於捕獲分析，請檢查以下文檔：

分析 Firepower 防火牆擷取，以有效針對網路問題進行疑難排解

4. FTD之間不相容的軟體 — FMC

FMC UI顯示：



建議的操作

檢查FTD /ngfw/var/log/messages檔案：

<#root>

```
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_connections [INFO] Need to send SW
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_channel [INFO] >> ChannelState do_d
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_heartbeat [INFO] Saved SW VERSION f
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:ssl_mac [WARN]

FMC(manager) 10.62.148.247 send unsupported version 10.10.0.4

Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_connections [INFO] <<<<<<<<<<<<<<<<
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:stream_file [INFO] Stream CTX destroye
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_channel [INFO] >> ChannelState Shut
```

檢查Firepower相容性矩陣：

[思科Firepower相容性指南]

5. FTD和FMC之間的時間差異

FTD-FMC通訊對兩個裝置之間的時間差異非常敏感。要求同一NTP伺服器同步FTD和FMC。

具體來說，當FTD安裝在41xx或93xx等平台時，其時間設定會取自父機箱(FXOS)。

建議的操作

確保機箱管理器(FCM)和FMC使用相同的時間源（NTP伺服器）

6. sftunnel進程關閉或禁用

在FTD上，sftunnel 程式會處理註冊程式。這是Manager配置之前的進程狀態：

<#root>

>

pmtool status
…
sftunnel

(system) -

Waiting
Command:

/ngfw/usr/local/sf/bin/sftunnel -d -f /etc/sf/sftunnel.conf
PID File: /ngfw/var/sf/run/sftunnel.pid
Enable File: /ngfw/etc/sf/sftunnel.conf
CPU Affinity:
Priority: 0
Next start: Mon Apr 20 06:12:06 2020
Required by: sfmgr,sfmbservice,sfipproxy
CGroups: memory=System/ProcessHigh

註冊狀態：

<#root>

>

show managers

No managers configured.

配置管理器：

```
<#root>

>

configure manager add 10.62.148.75 cisco123

Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

現在進程已啟動：

```
<#root>

>

pmtool status
…
sftunnel

 (system) -

Running

 24386
Command: /ngfw/usr/local/sf/bin/sftunnel -d -f /etc/sf/sftunnel.conf
PID File: /ngfw/var/sf/run/sftunnel.pid
Enable File: /ngfw/etc/sf/sftunnel.conf
CPU Affinity:
Priority: 0
Next start: Mon Apr 20 07:12:35 2020
Required by: sfmgr,sfmbservice,sfipproxy
CGroups: memory=System/ProcessHigh(enrolled)
```

在某些情況下，進程可能會關閉或禁用：

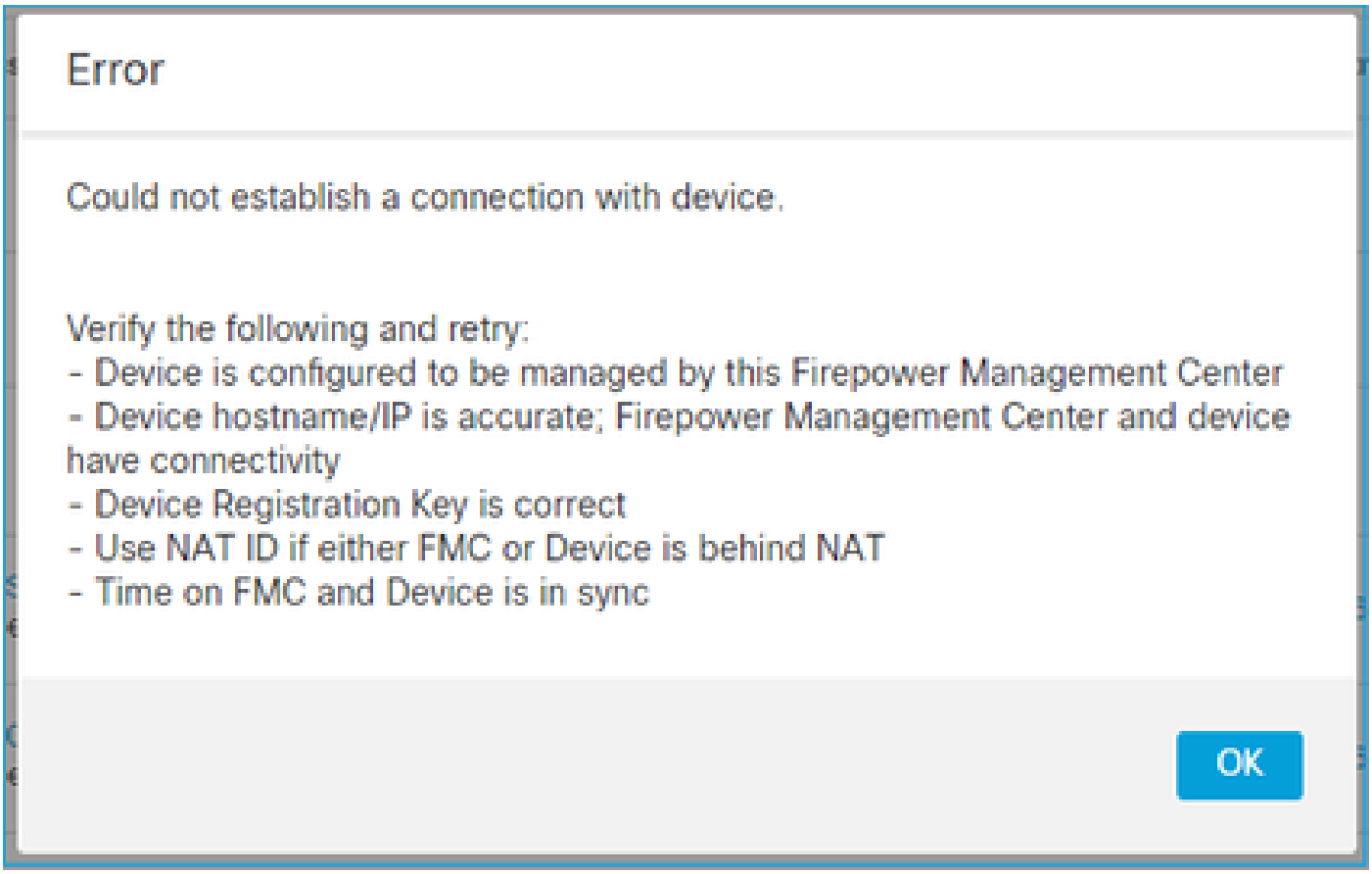
```
<#root>

>

pmtool status
…
sftunnel

 (system) -

User Disabled

Command: /ngfw/usr/local/sf/bin/sftunnel -d -f /etc/sf/sftunnel.conf
```

```
PID File: /ngfw/var/sf/run/sftunnel.pid
Enable File: /ngfw/etc/sf/sftunnel.conf
CPU Affinity:
Priority: 0
Next start: Mon Apr 20 07:09:46 2020
Required by: sfmgr,sfmbservice,sfipproxy
CGroups: memory=System/ProcessHigh
```

管理器狀態看起來正常：

```
<#root>

>

show managers

Host                          : 10.62.148.75
Registration Key              : ****

Registration                  : pending

RPC Status                    :
```

另一方面，裝置註冊失敗：



在FTD上，/ngfw/var/log/messages中看不到任何相關訊息

建議的操作

收集FTD疑難排解檔案並聯絡Cisco TAC

7. FTD有待於輔助FMC註冊

在某些情況下，初始FTD註冊到FMC HA設定後，FTD裝置不會新增到輔助FMC。

建議的操作

使用本檔案所述的程式：

使用CLI解決Firepower管理中心高可用性中的裝置註冊

警告：此過程是入侵性的，因為它包含裝置取消註冊。這會影響FTD裝置組態（已刪除）。建議僅在初始FTD註冊和設定期間使用此程式。在不同情況下收集FTD和FMC疑難排解檔案，並與Cisco TAC聯絡。

8.由於路徑MTU導致註冊失敗

在Cisco TAC中可看到的情況中，sftunnel流量必須經過具有小MTU的鏈路。sftunnel資料包具有Don't fragment bit Set，因此不允許分段：

	Source	Destination	Protocol	Length	TCP Segment	Don't fragment	Info
57	10.62.148.75	10.62.148.42	TCP	74	0	Set	47709 → 8305 [SYN] Seq=2860693630 Win=29200 Len=0 MS
58	10.62.148.42	10.62.148.75	TCP	74	0	Set	8305 → 47709 [SYN, ACK] Seq=279535377 Ack=2860693631
59	10.62.148.75	10.62.148.42	TCP	66	0	Set	47709 → 8305 [ACK] Seq=2860693631 Ack=279535378 Win=
60	10.62.148.75	10.62.148.42	TLSv1.2	229	163	Set	Client Hello
61	10.62.148.42	10.62.148.75	TCP	66	0	Set	8305 → 47709 [ACK] Seq=279535378 Ack=2860693794 Win=
62	10.62.148.42	10.62.148.75	TLSv1.2	1514	1448	Set	Server Hello
63	10.62.148.75	10.62.148.42	TCP	66	0	Set	47709 → 8305 [ACK] Seq=2860693794 Ack=279536826 Win=
64	10.62.148.42	10.62.148.75	TLSv1.2	803	737	Set	Certificate, Certificate Request, Server Hello Done
65	10.62.148.75	10.62.148.42	TCP	66	0	Set	47709 → 8305 [ACK] Seq=2860693794 Ack=279537563 Win=
66	10.62.148.75	10.62.148.42	TLSv1.2	2581	2515	Set	Certificate, Client Key Exchange, Certificate Verify
67	10.62.148.42	10.62.148.75	TCP	66	0	Set	8305 → 47709 [ACK] Seq=279537563 Ack=2860696309 Win=
68	10.62.148.42	10.62.148.75	TLSv1.2	1284	1218	Set	New Session Ticket, Change Cipher Spec, Encrypted Ha
69	10.62.148.75	10.62.148.42	TLSv1.2	364	298	Set	Application Data
70	10.62.148.42	10.62.148.75	TLSv1.2	364	298	Set	Application Data

此外，在/ngfw/var/log/messages檔案中，您可以看到如下消息：

MSGS: 10-09 14:41:11 ftd1 SF-IMS[7428]: [6612] sftunneld:sf_ssl [ERROR] Connect:SSL握手失敗

建議的操作

驗證分段是否會導致封包遺失，請在FTD、FMC上擷取，並在路徑中的裝置上理想地擷取。檢查是否看到兩端都到達的資料包。

在FTD上，降低FTD管理介面的MTU。預設值為1500位元組。MAX對於管理介面為1500，對於事件介面為9000。此命令是在FTD 6.6版中新增的。

Cisco Firepower威脅防禦命令參考

範例

<#root>

>

configure network mtu 1300

MTU set successfully to 1300 from 1500 for eth0
Refreshing Network Config...
Interface eth0 speed is set to '10000baseT/Full'

驗證

<#root>

>

show network

```
===============[ System Information ]===============
Hostname                  : ksec-sfvm-kali-3.cisco.com
DNS Servers               : 192.168.200.100
Management port           : 8305
IPv4 Default route
  Gateway                 : 10.62.148.1
  Netmask                 : 0.0.0.0


======================[ eth0 ]======================
State                     : Enabled
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1300
MAC Address               : 00:50:56:85:7B:1F
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.62.148.42
Netmask                   : 255.255.255.128
Gateway                   : 10.62.148.1
----------------------[ IPv6 ]----------------------
```

若要驗證來自FTD的路徑MTU，您可以使用以下命令：

<#root>

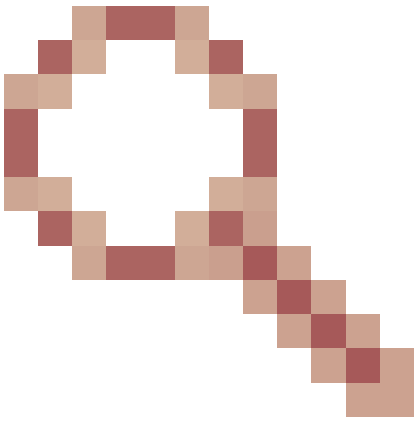
```
root@firepower:/home/admin#
ping -M do -s 1472 10.62.148.75
```

do 選項會設定ICMP封包中的「不分段」位元。此外，當您指定1472時，裝置會傳送1500位元組：（IP標頭= 20位元組）+（ICMP標頭= 8位元組）+（1472位元組ICMP資料）

在FMC上，降低FMC管理介面上的MTU值（如本檔案所述）：

配置Firepower管理中心管理介面

9.從機箱管理器UI進行載入程式更改後，FTD將取消註冊



這適用於FP41xx和FP93xx平台，並記錄在Cisco錯誤ID CSCvn45138

.

一般情況下，除非執行災難恢復，否則不能從機箱管理器(FCM)進行載入程式更改。

建議的操作

如果您進行載入程式更改並且匹配條件（FTD-FMC通訊中斷，而FTD在載入程式更改後啟動），則必須刪除並重新將FTD註冊到FMC。

10.由於ICMP重新導向訊息，FTD失去對FMC的存取許可權

此問題可能影響註冊過程或在註冊後中斷FTD-FMC通訊。

此案例中的問題在於網路裝置將ICMP重新導向訊息傳送到FTD管理介面和黑洞FTD-FMC通訊。

如何識別此問題

在本例中，10.100.1.1是FMC IP地址。在FTD上，由於FTD在管理介面上收到的ICMP重新導向訊息，存在快取路由：

```
<#root>

ftd1:/ngfw/var/common#

ip route get 10.100.1.1

10.100.1.1 via 10.10.1.1 dev br1  src 10.10.1.23

cache
```

建議的操作

步驟 1

在傳送它的裝置（例如上游L3交換器、路由器等）上停用ICMP重新導向。

步驟 2

從FTD CLI清除FTD路由快取：

```
<#root>

ftd1:/ngfw/var/common#

ip route flush 10.100.1.1
```

如果沒有重新導向，則如下所示：

```
<#root>

ftd1:/ngfw/var/common#

ip route get 10.100.1.1

10.100.1.1 via 10.62.148.1 dev eth0  src 10.10.1.23
    cache  mtu 1500 advmss 1460 hoplimit 64
```

參考資料

- 瞭解ICMP重新導向訊息
- 思科錯誤ID CSCvm53282 FTD：由ICMP重定向新增的路由表將永久停滯在路由表快取中

相關資訊

- NGFW配置指南

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。